Van hype naar aanpak

De digitale snelweg biedt veel kansen, maar ook grote risico's. Steeds opnieuw worden cyber incidenten in de media gemeld. Voor elke online organisatie geldt niet zozeer de vraag of men wordt gehackt, maar wanneer en hoe vaak.

Cybersecurity hoort daarom op elke bestuursagenda te staan. Het bestuur moet het goede voorbeeld geven en de juiste vragen stellen. Dat is de belangrijkste boodschap van de in mei 2016 verschenen publieke managementletter (PML) van de NBA met alt titel 'Van hype naar aanpak'.

Vijf signalen en aanbevelingen

In de PML staan **vijf signalen** centraal:

1. Onderwerp voor de bestuurskamer
2. Het draait om de kroonjuwelen
3. De zwakste schakel
4. Incasseren en reageren
5. De jaarrekening bestaat uit bytes

De betrouwbaarheid van alle informatie in de jaarrekening is afhankelijk van de integriteit van de onderliggende data. Daarom dient databeveiliging voorop te staan. Maar ook hier ligt het primaat in de bestuurskamer. Bestuurders moeten cybersecurity inbedden in hun

strategie en risicobeleid, verankeren in hun organisatie. Elke bestuurder moet zich realiseren dat cybercrime een van de grotere risico's is die een organisatie kunnen bedreigen. Net als fraude of brand. De accountant kan bijdragen aan de bewustwording, door de juiste vragen over cybersecurity stellen aan bestuurders en toezichthouders. Uiteraard zal hij (of zij) cybersecurity een passende plaats in de controle geven.

Alles beveiligen is onmogelijk. Daarom dient de focus op de kroonjuwelen gelegd te worden: de meest vitale data en processen. De mens is vaak de zwakste schakel, ook cultuur en gedrag verdienen de aandacht. Het gaat er in essentie om dat een organisatie over voldoende digitale weerbaarheid beschikt: incasseringsvermogen en slagkracht.

Elk signaal leidt tot een bijbehorende **aanbeveling**:

1. Stel als bestuurder de juiste vragen
2. Breng de kroonjuwelen in kaart
3. Besteed ook aandacht aan cultuur en gedrag
4. Vergroot de digitale weerbaarheid
5. Zorg voor voldoende cyber kennis bij de controle

Van hype naar aanpak

Cybercrime, de tegenhanger van cybersecurity, is big business. Malafide organisaties verdienen veel geld door organisaties te hacken. Het idee dat alleen grote, internationale ondernemingen het slachtoffer worden klopt niet. Mkb-bedrijven, organisaties van maatschappelijk belang (zoals gemeenten, ziekenhuizen en energiebedrijven) en ook particulieren worden getroffen door cybercrime. Weliswaar is hun risicoprofiel anders, maar de dreiging is er net zo goed. Het is eigenlijk niet meer de vraag of je wordt gehackt, maar wanneer en hoe vaak. Absolute veiligheid bestaat niet.

De gevolgen van een cyberaanval kunnen verstrekkend zijn. Niet alleen door directe schade tijdens een hack, maar ook indirect. Diefstal van intellectueel eigendom, verlies van klanten en omzet, reputatieschade, claims van gedupeerden of boetes van externe toezichthouders. Aanvullend zijn er kosten voor (forensisch) onderzoek, juridisch advies en het herstel van de aangerichte schade.

Met de juiste aanpak kan veel schade worden voorkomen. De oplossing ligt niet alleen in de techniek. Het gaat er veel meer om hoe cybersecurity in de hele organisatie is ingebed. Bestuurder, werknemer, toezichthouder, interne en openbare accountant spelen allemaal een rol. Er moet aandacht zijn voor de kroonjuwelen, cultuur en gedrag, bewustwording en opleiding. De digitale weerbaarheid moet omhoog, het vermogen om te incasseren en snel te reageren.

Cybersecurity raakt de accountant vanuit verschillende routes. Vanuit zijn controleperspectief moet hij zich realiseren dat de basis voor de jaarrekening bestaat uit bytes. De betrouwbaarheid van de informatie is afhankelijk van de integriteit van de onderliggende data. De rol van de accountant gaat daarom verder dan het vaststellen dat de schade van een cyberincident getrouw in de jaarrekening is verwerkt of dat de

continuïteit is gewaarborgd. De belangrijkste rol voor de accountant ligt misschien wel in zijn natuurlijke adviesfunctie: het stellen van de juiste vragen over cybersecurity. Vaststellen dat er bij bestuur en toezichthouders voldoende awareness bestaat, toetsen of cybersecurity de juiste plaats heeft in de strategie en het risicobeleid.

Download

Van hype naar aanpak : publieke managementletter over cybersecurity	PDF 3,35 MB
From hype to policy (2016)	PDF 3,51 MB
Presentatie Jacques Urlus - Cybercrime	PDF 462,29 kB
Presentatie Gerard van IJzendoorn - Datalekken en de accountant	PDF 679,86 kB